JOURNAL OF NUMBER THEORY 1, 179–194 (1969)

Simultaneous Asymptotic Diophantine Approximations to a Basis of a Real Cubic Number Field*

WILLIAM W. ADAMS

Department of Mathematics,
University of California, Berkeley, California 94720

Communicated by Hans Zassenhaus

Received August 5, 1968

The units in cubic number fields together with the uniform distribution theorem are used to prove the following theorem. Let $1, \beta_1, \beta_2$ be a basis for a real cubic number field. Let $C > 0$ be a given constant. Let λ_B equal the number of solutions in integers q, p_1, p_2 of the inequalities $0 < q\beta_i - p_i < C/q^{1/2}$ $(i = 1, 2)$, $1 \leq q \leq B$. Then $\lambda_B = O(1)$ or there is a constant $C' > 0$ such that $\lambda_B \sim C' \log B$ $(B \to \infty)$. The stumbling blocks for generalizing this result to higher dimensions are discussed.

1. INTRODUCTION

Let $\beta_1, \ldots, \beta_n$ be n real numbers. Let $\psi(q) > 0$ be a decreasing function (as $q \to \infty$) and set $\omega(q) = q\psi(q)^n$. Let $\lambda_B(\beta_1, \ldots, \beta_n, \omega)$ be the number of solutions in integers $q, p_1, \ldots, p_n$ of the inequalities

$$0 < q\beta_i - p_i < \psi(q) \qquad (i = 1, \ldots, n)$$
$$1 \leq q \leq B.$$

It is known [8] that for almost all $(\beta_1, \ldots, \beta_n)$,

$$\lambda_B(\beta_1, \ldots, \beta_n, \omega) \sim \int_1^B \psi(t)^n \, dt \qquad (B \to \infty). \tag{A}$$

Thus there is the problem of deciding, for a specifically given n-tuple, whether this result is valid.

Let $1, \beta_1, \ldots, \beta_n$ be a basis of a real algebraic number field of degree $m = n+1$. Schmidt [9] showed that if $\omega(q)$ tends to infinity then (A) does indeed hold (see also [1], [6]). It is well known ([3]; page 79) that if

* This research was partially supported by National Science Foundation grant CP-3990.

$\omega(q) \equiv C$ and C is sufficiently small, then there are only finitely many solutions and so (A) is not valid in this case. There is then the problem of computing asymptotically the number of solutions when $\omega(q) \equiv C$ and C is large enough to guarantee an infinite number of them. Lang [6] showed in the case that $m = 2$, that (A) holds but with a constant C' depending *discretely* on C in front of the integral. Thus the abnormality of these n-tuples for small C persists for larger C, although in a mild form.

It is the purpose of this paper to prove the corresponding result when $m = 3$. In Section **6** we indicate (in the totally real case) what the missing ingredients are for generalizing the result to higher dimensions.

Specifically we prove

THEOREM 1. *Let $1, \beta_1, \beta_2$ be a basis for a real cubic number field. Let $C > 0$ be a given constant. Let $\lambda_B = \lambda_B(\beta_1, \beta_2, C)$ equal the number of solutions in integers q, p_1, p_2 of the inequalities*

$$* \qquad 0 < q\beta_1 - p_1 < C/q^{1/2}, \quad 0 < q\beta_2 - p_2 < C/q^{1/2}$$

$$** \qquad 1 \leq q \leq B.$$

Then either $\lambda_B = O(1)$ or there is a constant $C' > 0$ such that

$$\lambda_B \sim C' \log B \qquad (B \to \infty).$$

Of course if $C \geq 1$ then λ_B is not bounded. There is a dual theorem.

THEOREM 2. *Let β_1, β_2, C be as in Theorem 1. Let Λ_B equal the number of solutions in integers q_1, q_2, p of the inequalities*

$$0 < q_1\beta_1 + q_2\beta_2 - p < C/q^2$$

$$1 \leq q_1, q_2 \leq B$$

where $q = \max(q_1, q_2)$. Then either $\Lambda_B = O(1)$ or there is a constant $C'' > 0$ such that

$$\Lambda_B \sim C'' \log B \qquad (B \to \infty).$$

We prove Theorem 1 only; the proof of Theorem 2 is similar. The proof follows Lang's scheme [6] of looking at the norm of certain elements in the number field and in that way reducing the problem to counting units in the field. But here we cannot count all the units or even some obvious subset of them; we must show that the uniform distribution theorem ([3]; page 64) applies to the conditions we have.

Lang, in his theorem, was able to give an error term of $O(1)$. We give no error term. This is because none is known in the uniform distribution theorem for the numbers we apply it to. They are the log or ratio

of logs of certain algebraic numbers. This is further discussed in Section 7. Also one of the major stumbling blocks to generalizing the result to higher dimensions is the verification of the hypothesis of the associated uniform distribution theorem.

The proof breaks up into two cases. Let K be the field of Theorem 1.

(I) K is totally real.
(II) K has a complex embedding.

These numbers for the cases will be used from now on.

We denote by $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ the rational integers, rational numbers, real numbers and complex numbers respectively. $C_1, C_2, \ldots$ and $c_1, c_2 \ldots$ denote constants depending only on the initial data. The phrase "sufficiently large" means larger than an unspecified but easily computable constant depending only on the initial data.

2. The Reduction to Counting Units

Let $\tau_0 =$ identity, τ_1, τ_2 denote the three distinct embeddings of K into $\mathbf{C}$. Set, for $\alpha \in K$, $\tau_i \alpha = \alpha^{(i)}$ (i $= 0, 1, 2$). (So in Case II, $\alpha^{(2)} = \overline{\alpha^{(1)}}$ —where the bar denotes complex conjugation). We take from Schmidt [9] the following lemma.

Lemma 1. *There is a basis $\alpha_0, \alpha_1, \alpha_2$ of $K/\mathbf{Q}$ such that*

$$\alpha_0^{(i)} + \alpha_1^{(i)}\beta_1 + \alpha_2^{(i)}\beta_2 = 0 \qquad (i = 1, 2) \tag{1}$$

$$A = \begin{pmatrix} \alpha_1^{(1)} & \alpha_2^{(1)} \\ \alpha_1^{(2)} & \alpha_2^{(2)} \end{pmatrix} \quad \text{is nonsingular.} \tag{2}$$

$$\alpha_0 + \alpha_1\beta_1 + \alpha_2\beta_2 = 1. \tag{3}$$

Proof. From ([5]; page 4) we have that

$$\langle \alpha, \beta \rangle = Tr_{\mathbf{Q}}^{K}(\alpha\beta), \qquad \text{for } \alpha, \beta \in K,$$

is a nondegenerate bilinear form on K as a $\mathbf{Q}$ space. So let $\alpha_0, \alpha_1, \alpha_2$ be the associated dual basis of $K/\mathbf{Q}$ of $1, \beta_1, \beta_2$. Let A_1 be the matrix with rows

$$(\alpha_0^{(i)}, \alpha_1^{(i)}, \alpha_2^{(i)}) \qquad (i = 0, 1, 2)$$

and B_1 be the matrix with rows

$$(\beta_0^{(i)}, \beta_1^{(i)}, \beta_2^{(i)}) \qquad (i = 0, 1, 2).$$

Then we have in particular $A_1^t B_1 = I$ ($I =$ identity matrix, t denotes the transpose matrix). Since $(A_1^t)^{-1} = (A_1^{-1})^t$ we have $A_1 B_1^t = I$. This last relation gives (1) and (3). Finally (2) follows since extending τ_0, τ_1, τ_2

to the normal closure of $K/\mathbf{Q}$ we see they permute the rows of A_1 in such a way that all possible 2×2 minors defined by the last two columns of A_1 appear in the place of A in A_1, so one of them nonsingular implies they all are, hence A is nonsingular. This completes the proof of Lemma 1.

Let M be the free $\mathbf{Z}$-module of rank 3 generated by $\alpha_0, \alpha_1, \alpha_2$. So for $\xi \in M$ write

$$\xi = q\alpha_0 + p_1\alpha_1 + p_2\alpha_2$$

with $q, p_1, p_2 \in \mathbf{Z}$. We view M as being in 1–1 correspondence with the possible solutions of *. Now for $i = 1, 2$ we have

$$\xi^{(i)} = q\alpha_0^{(i)} + p_1\alpha_1^{(i)} + p_2\alpha_2^{(i)}$$

and so by (1) for $i = 1, 2$

$$-\xi^{(i)} = \alpha_1^{(i)}(q\beta_1 - p_1) + \alpha_2^{(i)}(q\beta_2 - p_2). \tag{4}$$

Now let $\mathfrak{o}$ be the order associated with M (see [2]; page 88); that is

$$\mathfrak{o} = \{\alpha \in K : \alpha M \subseteq M\}.$$

Clearly $\mathfrak{o}$ is a subring of the integers of K, of rank 3 as a $\mathbf{Z}$-module. Let U be the group of units of $\mathfrak{o}$. Define an equivalence relation in M by:

$\xi_1 \sim \xi_2$ if and only if there is a $\zeta \in U$ such that $\xi_1 = \zeta\xi_2$ for $\xi_1, \xi_2 \in M$.

If $\Omega \subseteq M$ is an equivalence class, then for all $\xi \in \Omega$, $|\mathbf{N}\xi|$ is the same and we denote this value by $\mathbf{N}\Omega$ ($\mathbf{N}$ denotes the "norm" of $K/\mathbf{Q}$).

LEMMA 2. *There are at most a finite number of classes $\Omega \subseteq M$ which yield solutions to **.

Proof. We first recall the well known fact (see [2]; page 90) that there are only finitely many classes Ω in M with $\mathbf{N}\Omega$ below a given value. Thus it suffices to show that if $\xi \in M$ satisfies * then ξ has bounded norm. By * and (4)

$$|\mathbf{N}\xi| = |\xi||\xi^{(1)}||\xi^{(2)}| \leq |\xi|(c_1/q) < c_2$$

(note that * is used for both of the last two inequalities). So Lemma 2 is proved.

Hence it suffices to show the following:

*Let $\Omega \subseteq M$ be a fixed equivalence class. Then the number of $\xi \in \Omega$ yielding solutions to * and ** is either bounded or asymptotic to $C_1 \log B$ $(B \to \infty)$ for some $C_1 > 0$.*

Now from the Dirichlet theorem ([2]; page 112) we know that U has the following form: in Case

(I) there are two multiplicatively independent units $\zeta_1, \zeta_2 > 1$ in U such that

$$U = \{\pm\zeta_1^{v_1}\zeta_2^{v_2}\} \qquad (v_1, v_2 \in \mathbf{Z}),$$

(II) there is a $\zeta_1 > 1$ in U such that

$$U = \{\pm\zeta_1^{v_1}\} \qquad (v_1 \in \mathbf{Z}).$$

In both cases we write a typical element of U in the form ζ^v (so in Case I v is the vector (v_1, v_2) and in Case II $v = v_1$). So letting $\xi_0 > 0$ be any element of Ω, we have

$$\Omega = \{\pm\zeta^v\xi_0\} \qquad ((\mathrm{I})\ v \in \mathbf{Z}^2 \quad \text{or} \quad (\mathrm{II})\ v \in \mathbf{Z}).$$

Hence we must see which units satisfy * and **.

3. Setting up the Uniform Distribution Problem

We continue with the notation of the previous section. If $S \subseteq M$ is a subset, set $\lambda_B(S)$ = number $\xi \in S$ satisfying * and **. We will concern ourselves with $\lambda_B(\Omega^+)$, where $\Omega^+ = \{\zeta^v\xi_0\}$, the positive elements of Ω. The negative elements, Ω^-, in Ω would correspond to negative denominators in * and hence as we will show in Lemma 5, $\lambda_B(\Omega^-) = O(1)$.

We will need

Lemma 3: *There are only finitely many* $\xi = q\alpha_0 + p_1\alpha_1 + p_2\alpha_2 \in \Omega$ *with* $q = 0$.

Proof. Suppose $q = 0$. Then

$$\mathrm{N}\Omega = |\mathrm{N}\xi| = |f(p_1, p_2)|$$

is fixed, where f is a homogeneous polynomial of degree 3 in 2 variables with rational coefficients. It is a well known theorem of Thue (see [7]; page 154) that this equation can be satisfied for at most a finite number of p_1, p_2.

We must now set up some notation. Let $\xi_v = \zeta^v\xi_0$ be a typical element of Ω^+. Write

$$\xi_v = q_v\alpha_0 + p_{1v}\alpha_1 + p_{2v}\alpha_2.$$

Set

$$\gamma_{iv} = q_v\beta_i - p_{iv} \qquad (i = 1, 2). \tag{5}$$

Then we have derived before, (4),

$$(\xi_v^{(1)}, \xi_v^{(2)})^t = -A(\gamma_{1v}, \gamma_{2v})^t \tag{6}$$

where A is given in (2). Set

$$\delta_{iv} = q_v^{1/2}\gamma_{iv} \qquad (i = 1, 2)$$

for $q_\nu > 0$. Then $\lambda_B(\Omega^+)$ = number of $\xi_\nu \in \Omega^+$ such that

$$0 < \delta_{1\nu}, \delta_{2\nu} < C \tag{7}$$

$$1 \leq q_\nu \leq B. \tag{8}$$

Now for $q_\nu \neq 0$ set

$$\kappa'_\nu = \alpha_0 + \frac{p_{1\nu}}{q_\nu}\alpha_1 + \frac{p_{2\nu}}{q_\nu}\alpha_2$$

(so for q_ν large and (7) holding, κ'_ν is close to 1—see (3)). We have

$$\xi_\nu = q_\nu \kappa'_\nu \tag{9}$$

and

$$\kappa'_\nu = 1 + \frac{\varepsilon_\nu}{q_\nu} \tag{10}$$

where

$$\varepsilon_\nu = \alpha_1\gamma_{1\nu} + \alpha_2\gamma_{2\nu}. \tag{11}$$

Now $\xi_\nu = \zeta^\nu \xi_0 = q_\nu \kappa'_\nu$ so for $q_\nu > 0$

$$\delta_{i\nu} = q_\nu^{1/2}\gamma_{i\nu} = \xi_0^{1/2}\kappa_\nu'^{-1/2}\zeta^{\nu/2}\gamma_{i\nu} \qquad (i = 1, 2). \tag{12}$$

Set

$$\eta_{i\nu} = \zeta^{\nu/2}\gamma_{i\nu} \qquad (i = 1, 2) \tag{13}$$

and

$$\kappa_\nu = \xi_0^{1/2}\kappa_\nu'^{-1/2} \tag{14}$$

and we obtain

$$\delta_{i\nu} = \kappa_\nu \eta_{i\nu} \qquad (i = 1, 2). \tag{15}$$

LEMMA 4. *Let* $\lambda_B^1(\Omega^+)$ *be the number of solutions to* (i), (ii), (iii) *and* (iv) *below*:

(i) ξ_ν *is sufficiently large*

(ii) $|\eta_{1\nu}|, |\eta_{2\nu}| \leq 10\xi_0^{-1/2}C = C_2$

(iii) $0 < \eta_{1\nu}, \eta_{2\nu} < C\kappa_\nu^{-1}$

(iv) $1 \leq \xi_\nu \leq 2B$.

Then

$$\lambda_B(\Omega^+) + O(1) \leq \lambda_B^1(\Omega^+) \leq \lambda_{4B}(\Omega^+) + O(1).$$

Proof. We first note that by (i) and Lemma 3 we have $q_\nu \neq 0$. Then from (i) and the definition $\xi_\nu = \zeta^\nu \xi_0$ of ξ_ν we have that ζ^ν is large, so by (ii) and (13) we have $\gamma_{i\nu}$ is small (i = 1, 2). So by (11) ε_ν is small and thus from (10) we may assume

$$\tfrac{1}{2} \leq \kappa'_\nu \leq 3/2 \quad (q_\nu \neq 0 \text{ implies } |q_\nu| \geq 1).$$

From this and (9) we have in fact that q_ν is large and positive. In this

situation (15) yields that (iii) is equivalent to (7). And finally, by (iv)

$$q_\nu = \xi_\nu \kappa_\nu'^{-1} \leq 2\kappa_\nu'^{-1} B \leq 4B.$$

This all shows that with a bounded number of exceptions all the ξ_ν satisfying (i)–(iv) of the lemma satisfy (7) and (8) with the B in (8) replaced by $4B$; hence the right hand inequality is true.

Conversely assume (7) and (8). Then with a bounded error we may assume q_ν is large. So from (7), (10), (11) and (12) we see κ_ν' is close to 1 and so by (9) ξ_ν is large. Again by (15), (iii) and (7) are equivalent. Thus from the above and (iii) we have (ii) is true. Finally using (8)

$$\xi_\nu = q_\nu \kappa_\nu' \leq 2q_\nu \leq 2B$$

using the fact that κ_ν' is close to 1. Thus the lemma is proved.

We also obtain

LEMMA 5. $\lambda_B(\Omega^-) = O(1)$.

Proof. This follows the proof of Lemma 4. Namely, again we may assume q_ν is large, so again κ_ν' is close to 1 and so by (9) $\xi_\nu > 0$. But in Ω^-, $\xi_\nu = -\zeta^\nu \xi_0 < 0$ (we chose $\xi_0 > 0$).

COROLLARY. *It suffices to show that*

$$\lambda_B^1(\Omega^+) \sim C_1 \log B.$$

Proof. This is immediate from Lemmas 4, 5 and the statement following the proof of Lemma 2.

4. THE UNIFORM DISTRIBUTION PROBLEM

One essential point in the proof of our theorem is that we may view κ_ν as a constant. In this section we apply the uniform distribution theorem to count when in Lemma 4, (iii) $C\kappa_\nu^{-1}$ is replaced by a constant, and then we show that this is all right. Here, however, we change our parameter from B to ν_1 and then in the next section put the B back. First we need the following lemma to guarantee the irrationality of certain quantities.

LEMMA 6. *Let $\alpha \in K$ be any irrational element. Then $\alpha\alpha^{(1)^2} \neq 1$.*

Proof. Assume that $\alpha\alpha^{(1)^2} = 1$. Let G be the galois group of the splitting field of $K/\mathbf{Q}$. Since α is irrational, $K = \mathbf{Q}(\alpha)$ ($[K: \mathbf{Q}] = 3$, a prime) and so G can be viewed as a subgroup of the permutation group of $\alpha, \alpha^{(1)}, \alpha^{(2)}$. Moreover the order of G is 3 or 6 and hence G must contain the 3-cycle

$(\alpha, \alpha^{(1)}, \alpha^{(2)})$. Applying this to our relation we get

$$\alpha\alpha^{(1)2} = \alpha^{(1)}\alpha^{(2)2} = \alpha^{(2)}\alpha^2 = 1.$$

These may be solved to yield $\alpha^9 = 1$. Since K is real, $\alpha = \pm 1$ contradicting the irrationality of α.

LEMMA 7. Let $\#'_N$ *be the number of solutions of the inequalities*

$$0 < \eta_{1v}, \eta_{2v} < C_3 \tag{16}$$

and

$$1 \leq v_1 \leq N.$$

Then

$$\#'_N \sim C_4 N \qquad (N \to \infty)$$

where $C_4 > 0$ *is some constant. The similar statement holds for* (16) *and*

$$1 \leq -v_1 \leq N.$$

Proof. We prove only the first statement.

With A as in (2), set $A_2 = -\xi_0^{-1}A$. Then from (6) and (13) we have

$$A_2(\eta_{1v}, \eta_{2v})^t = (\rho_{1v}, \rho_{2v})^t \tag{17}$$

where

$$\rho_{iv} = \zeta^{v/2}\zeta^{(i)v} \qquad (i = 1, 2).$$

We now must consider the two cases separately.

(I) So K is totally real. Let $\varphi: \mathbf{R}^2 \to \mathbf{R}^2$ be the linear map defined by A_2 (it is an isomorphism by Lemma 1). We wish to find the number of $(\eta_{1v}, \eta_{2v})^t$ lying in the square indicated in Figure 1. Applying φ to this

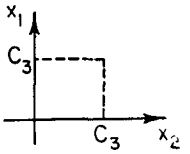

FIG. 1

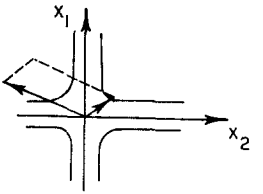

FIG. 2

region, we wish to find the number of $(\rho_{1v}, \rho_{2v})^t$ lying in some parallelogram—see Figure 2. Now

$$\rho_{1v}\rho_{2v} = (\mathbf{N}\zeta_1)^{v_1}(\mathbf{N}\zeta_2)^{v_2} = \pm 1$$

so these points are restricted to lie on one of the four branches of the hyperbolas $x_1x_2 = \pm 1$. Thus there are real numbers $0 < t_0 \leq t_1$ such that $(\rho_{1v}, \rho_{2v})^t$ lies in the parallelogram if and only if

$$t_0 < |\rho_{1v}| < t_1 \tag{18}$$

where t_0, t_1 depend only on which of the four branches the point lies. We note that we might have $t_0 = t_1$ so no points are counted, as in the branches with $x_1 < 0$ in Figure 2. So we have a number of cases depending on which curve we are on and this depends on the signs of ρ_{1v} and ρ_{2v}.

But first we manipulate (18) a little. It is true if and only if

$$\log t_0 < \log|\rho_{1v}| < \log t_1$$

or

$$\log t_0 < v_1 \log|\zeta_1^{1/2}\zeta_1^{(1)}| + v_2 \log|\zeta_2^{1/2}\zeta_2^{(1)}| < \log t_1.$$

Now

$$\log|\zeta_1^{1/2}\zeta_1^{(1)}| \quad \text{and} \quad \log|\zeta_2^{1/2}\zeta_2^{(1)}|$$

are linearly independent over $\mathbf{Q}$ since otherwise we would have a relation

$$\zeta_1^{v_1}\zeta_1^{(1)2v_1}\zeta_2^{v_2}\zeta_2^{(1)2v_2} = 1$$

for some integers v_1, v_2 not both zero. Then setting $\alpha = \zeta_1^{v_1}\zeta_2^{v_2}$ in Lemma 6 we have α is irrational since ζ_1, ζ_2 are independent units and $\alpha\alpha^{(1)^2} = 1$ and this contradicts Lemma 6.

Thus setting

$$\theta = (\log|\zeta_1^{1/2}\zeta_1^{(1)}|)/(\log|\zeta_2^{1/2}\zeta_2^{(1)}|)$$

we have θ is irrational and (18) is equivalent to

$$t_2 < v_1\theta + v_2 < t_3$$

for some obvious real numbers t_2, t_3 (which again may depend on which of the four curves the point lies).

Since θ is irrational we may apply the uniform distribution theorem to obtain the desired result. But we must be careful since t_2, t_3 may change with v_1, v_2; but they do so in a regular way. We note that

$$\rho_{1v} = \zeta_1^{v_1/2}\zeta_2^{v_2/2}\zeta_1^{(1)v_1}\zeta_2^{(1)v_2}$$

and so since $\zeta_1, \zeta_2 > 0$ the sign of ρ_{1v} depends only on the signs of $\zeta_1^{(1)v_1}$ and $\zeta_2^{(1)v_2}$. Similarly the sign of ρ_{2v} depends only on the signs of $\zeta_1^{(2)v_1}$ and $\zeta_2^{(2)v_2}$. In particular if v_1 and v_2 have a given parity then these signs are fixed and so the curve stays fixed. Hence there are four cases. For example if v_1 is even and v_2 is odd we wish to count the number of v_1', v_2' satisfying

$$t_2 < 2v_1'\theta + 2v_2' + 1 < t_3$$

for fixed t_2, t_3 or $(t_2-1)/2 \le v_1'\theta + v_2' < (t_3-1)/2$ where $1 \le v_1' \le N/2$. The uniform distribution theorem applies in all cases.

(II) So K has a complex embedding. Thus for all $\alpha \in K$, $\overline{\alpha^{(1)}} = \alpha^{(2)}$. In (17) we note that η_{1v}, η_{2v} are real and $\overline{\rho_{1v}} = \rho_{2v}$. Moreover the first row of A_2 is the complex conjugate of the second (see (2)).

Define $\varphi: \mathbf{R}^2 \to \mathbf{C}$ by composing A_2 with projection onto the first coordinate $\varphi: \mathbf{R}^2 \xrightarrow{A_1} \mathbf{C}^2 \xrightarrow{\text{proj.}} \mathbf{C}$. Then φ is $\mathbf{R}$-linear. Moreover φ is

nonsingular. To see this suppose

$$A_2 = \begin{pmatrix} a & b \\ \bar{a} & \bar{b} \end{pmatrix}$$

and $X = (x_1, x_2)^t \in \mathbf{R}^2$. Then $\varphi(X) = ax_1 + bx_2$. If $X \neq 0$ and $\varphi(X) = 0$ we would have $a/b \in \mathbf{R}$. In our case $a/b = \alpha_1^{(1)}/\alpha_2^{(1)}$ (and $b \neq 0$). Let $K^{(1)} = \tau_1 K$ (where $\tau_1 \alpha = \alpha^{(1)}$). Then $\varphi(X) = 0$ implies

$$\alpha_1^{(1)}/\alpha_2^{(1)} \in K^{(1)} \cap \mathbf{R} = \mathbf{Q}.$$

But $\alpha_0^{(1)}, \alpha_1^{(1)}, \alpha_2^{(1)}$ is a basis of $K^{(1)}/\mathbf{Q}$ so in particular $\alpha_1^{(1)}/\alpha_2^{(1)}$ is irrational. So φ is nonsingular as desired.

Again we wish to find the number of $(\eta_{1v}, \eta_{2v})^t$ lying in the square of Figure 1. Applying φ, we see we wish to find the number of ρ_{1v} lying in some parallelogram—see Figure 3. Now setting $\zeta_1 = \zeta$, $v_1 = v$ we recall

$$\rho_{1v} = \zeta^{v/2}\zeta^{(1)v}.$$

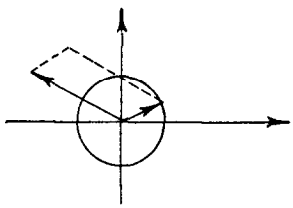

FIG. 3

Hence $|\rho_{1v}| = 1$ since

$$1 = |\mathbf{N}\zeta| = |\zeta\zeta^{(1)}\zeta^{(2)}| = |\zeta\zeta^{(1)}\overline{\zeta^{(1)}}| = |\zeta^{1/2}\zeta^{(1)}|^2.$$

Set $\rho_0 = \zeta^{1/2}\zeta^{(1)}$. So $|\rho_0| = 1$ and we wish to count the number of ρ_0^v lying in some nice subset of the unit circle in $\mathbf{C}$. Moreover by Lemma 6 ρ_0 is not a root of 1. So our result follows again from the uniform distribution theorem.

This completes the proof of Lemma 7.

LEMMA 8. *Let $\#_N$ be the number of solutions of* (i), (ii), (iii) *in Lemma 4 such that $1 \leq v_1 \leq N$. Then for some $C_5 > 0$*

$$\#_N \sim C_5 N \qquad (N \to \infty).$$

Also the result holds if we consider $1 \leq -v_1 \leq N$.

Proof. As in the proof of Lemma 4, (i), (ii) imply κ_v' is close to 1. In fact from (10) and (14)

$$\begin{aligned} C\kappa_v^{-1} &= C\xi_0^{-1/2}(1+\varepsilon_v/q_v)^{1/2} \\ &= C_6 + O(q_v^{-1}) \end{aligned}$$

where $C_6 = C\xi_0^{-1/2}$ and "O" is uniform in v (see the proof of Lemma 4). Hence we wish to count the number of v with ξ_v and q_v large and

$$0 < \eta_{1v}, \eta_{2v} < C_6 + O(q_v^{-1}) \tag{19}$$

and $1 \leq v_1 \leq N$.

We analyze the proof of Lemma 7. Let φ be as defined in each case there

$$\varphi: \mathbf{R}^2 \to \mathbf{R}^2 (= \mathbf{C}).$$

Let $\mathscr{B}$ be the square in $\mathbf{R}^2$

$$\mathscr{B}: 0 < x, y < C_6.$$

Then φ maps $\mathscr{B}$ into a parallelogram $\mathscr{P}$ and so maps $\mathscr{B} + O(q_v^{-1})$ into $\mathscr{P} + O(q_v^{-1})$ Hence we want to count the number of $v_1, 1 \leq v_1 \leq N$ such that

$$\varphi(\eta_{1v}, \eta_{2v}) \in \mathscr{P} + O(q_v^{-1}).$$

We applied, in Lemma 7, the uniform distribution theorem to certain sequences in certain intervals; these intervals are now perturbed by $O(q_v^{-1})$. Now clearly $q_v \to \infty$ (as $v_1 \to \infty$ yielding solutions), hence the next lemma suffices.

LEMMA 9. *Let y_v ($v = 1, 2, \ldots$) be a sequence of real numbers uniformly distributed* mod 1. *Let $x_v > 0$ be any sequence tending to zero.* Let I *be any interval contained in* $\mathbf{R}$ *of length* $|I|$. *Set F_N = number of v, m in $\mathbf{Z}$ such that $y_v + m \in I + O(x_v)$ and $1 \leq v \leq N$. Then $F_N \sim |I|N (N \to \infty)$.*

We note that if an error term had been given for the uniform distribution of the y_v and information had been given concerning how rapidly x_v tends to zero we could derive an error term for F_N.

Proof of Lemma 9. For any given $\varepsilon > 0$ there is an $N_0(\varepsilon)$ such that $n > N_0(\varepsilon)$ implies $x_v < \varepsilon$. Let I_ε = interval I increased on either side by length ε. Let $F_N(\varepsilon)$ = number of points $y_v + m \in I_\varepsilon$, $1 \leq v \leq N$. Then

$$F_N \leq F_N(\varepsilon) + N_0(\varepsilon)$$

and this is true for all N and ε. Hence as $N \to \infty$

$$\limsup F_N/N \leq \limsup (F_N(\varepsilon)/N + N_0(\varepsilon)/N) = |I_\varepsilon|,$$

since the y_v were assumed to be uniformly distributed. Since this is true for all $\varepsilon > 0$ we have

$$\limsup F_N/N \leq |I|.$$

The proof that $\liminf F_N/N \geq |I|$ is similar. This completes the proof of Lemma 9 and so of Lemma 8 also.

5. Proof of the Theorem

As noted in the last section, all that remains to be done to prove Theorem 1 is to take the result of Lemma 8, change the range $1 \leq \nu_1 \leq N$ (or $1 \leq -\nu_1 \leq N$) to $1 \leq \xi_\nu \leq 2B$, and show this gives

$$\lambda_B^1(\Omega^+) \sim C_1 \log B (C_1 > 0).$$

Hence we need to solve for ξ_ν in terms of ν_1.

Lemma 10. *There exists a constant $C_7 \neq 0$ such that for all ν satisfying conditions* (i), (ii) *and* (iii) *of Lemma 4 we have*

$$\log \xi_\nu = \nu_1 C_7 + O(1) \qquad (\nu_1 \to \pm\infty). \tag{20}$$

Proof. As noted in Lemma 8 the set of ν giving solutions to (i), (ii), (iii), is with a finite number of exceptions those giving a solution to (19). Since the validity of (20) for a sequence insures its validity for any subsequence, it suffices to show the following: Let $C_8 > 0$ be a constant. Then the set of ν such that

$$0 < \eta_{1\nu}, \eta_{2\nu} < C_8$$

satisfies (20).

Recall that $\xi_\nu = \zeta^\nu \xi_0$ and so it suffices to show (20) with ξ_ν replaced by ζ^ν. Now in Case II this is obvious since

$$\log \zeta^\nu = \log \zeta_1^{\nu_1} = \nu_1 \log \zeta_1.$$

So we restrict our attention to Case I. Examining the proof of Lemma 7 we see we have for all ν satisfying our conditions

$$\nu_1 \log \left|\zeta_1^{1/2}\zeta_1^{(1)}\right| + \nu_2 \log \left|\zeta_2^{1/2}\zeta_2^{(1)}\right| = O(1) \qquad (\nu_1 \to \pm\infty).$$

Hence

$$\begin{aligned}\log \zeta^\nu &= \nu_1 \log \zeta_1 + \nu_2 \log \zeta_2 \\ &= \nu_1 \log \zeta_1 - \left(\frac{\log \left|\zeta_1^{1/2}\zeta_1^{(1)}\right|}{\log \left|\zeta_2^{1/2}\zeta_2^{(1)}\right|} \nu_1 + O(1)\right) \log \zeta_2 \\ &= \nu_1 C_7 + O(1)\end{aligned}$$

where

$$C_7 = \log \zeta_1 - \frac{\log \left|\zeta_1^{1/2}\zeta_1^{(1)}\right|}{\log \left|\zeta_2^{1/2}\zeta_2^{(1)}\right|} \log \zeta_2.$$

Now $C_7 = 0$ implies

$$\det \begin{pmatrix} \log \zeta_1 & \log \zeta_2 \\ \log\left|\zeta_1^{(1)}\right| & \log\left|\zeta_2^{(1)}\right| \end{pmatrix} = 0$$

but this latter is the regulator of $\mathfrak{o}$ which is not zero ([2]; page 115).

COROLLARY. *ξ_v is large if and only if v_1 is large and has the same sign as C_7.*

We are now in a position to combine Lemmas 8 and 10 to complete the proof of Theorem 1. By the corollary of Lemmas 4 and 5 we must show

$$\lambda_B^1(\Omega^+) \sim C_1 \log B.$$

Also by the corollary above we may restrict the sign of v_1 to that of C_7.

Now let $N = |C_7|^{-1} \log B$. Then

$$1 \leq \xi_v \leq 2B$$

implies

$$0 \leq \log \xi_v \leq \log B + O(1)$$

implies by Lemma 10 and the definition of N

$$O(1) \leq v_1 C_7 \leq |C_7| N + O(1)$$

implies

$$O(1) \leq |v_1| \leq N + O(1).$$

Hence

$$\lambda_B^1(\Omega^+) \leq \#_{N+O_{(1)}}.$$

The lower bound is similar and so there are constants c_3, c_4 such that

$$\#_{N-c_3} \leq \lambda_B^1(\Omega^+) \leq \#_{N+c_4}.$$

Hence

$$\frac{\#_{N-c_3}}{N} \leq \frac{\lambda_B^1(\Omega^+)}{|C_7|^{-1} \log B} \leq \frac{\#_{N+c_4}}{N}.$$

Letting N (hence B) tend to infinity and using Lemma 8 we have

$$\lim_{B \to \infty} \frac{\lambda_B^1(\Omega^+)}{\log B} = C_1$$

where

$$C_1 = |C_7|^{-1} C_5, \text{ as desired.}$$

6. HIGHER DIMENSIONS

There are two basic problems with the generalization of this method to fields of degree > 3. It is the purpose of this section to discuss these problems. We will, however, restrict our attention to a *totally real* field K of degree $m = n+1$ over $\mathbf{Q}$. The notation set up before carries over in an obvious way to the present situation.

We first concern ourselves with Lemma 7, where the actual counting was done. We still would have

$$A_2(\eta_{1v}, \ldots, \eta_{nv})^t = (\rho_{1v}, \ldots, \rho_{nv})^t$$

where A_2 is a nonsingular matrix and

$$\rho_{iv} = \zeta^{v/n}\zeta^{(i)v} \qquad (i = 1, 2, \ldots, n)$$

and

$$\zeta^v = \zeta_1^{v_1} \ldots \zeta_n^{v_n}.$$

So we need to count the number of $(\rho_{1v}, \ldots, \rho_{nv})^t$ for $1 \leq v_1 \leq N$, lying in some parallelepiped in $\mathbf{R}^n$. Again

$$\rho_{1v} \ldots \rho_{nv} = \pm 1$$

and we may view our problem as that of computing the number of integers $v_1, \ldots, v_n$ such that $1 \leq v_1 \leq N$ and

$$v_1 X_1 + \ldots + v_n X_n$$

lies in some nice region in $\mathbf{R}^{n-1}$, where

$$X_i = \begin{pmatrix} \log \left|\zeta_i^{1/n}\zeta_i^{(1)}\right| \\ \vdots \\ \log \left|\zeta_i^{1/n}\zeta_i^{(n-1)}\right| \end{pmatrix} \qquad (i = 1, \ldots, n). \tag{21}$$

Let Λ be the additive abelian subgroup of $\mathbf{R}^{n-1}$ generated by $X_2, \ldots, X_n$. If Λ were a lattice then the problem would be to prove that $v_1 X_1$ is uniformly distributed mod Λ. This would be the case if the coordinates of X_1 with respect to $X_2, \ldots, X_n$ were linearly independent with 1 over $\mathbf{Q}$. A simple calculation shows that these conditions is the following conjecture:

CONJECTURE. *The n real numbers* $\det(X_2, \ldots, X_n)$, $\det(X_1, X_3, \ldots, X_n)$, $\ldots$, $\det(X_1, \ldots, X_{n-1})$ *are linearly independent over* $\mathbf{Q}$, *where the* X_i *are given by* (21), $\zeta_1, \ldots, \zeta_n > 1$ *are a basis of the units of the totally real field* K *and* $\alpha, \alpha^{(1)}, \ldots, \alpha^{(n)}$ *denote the conjugates of an* $\alpha \in K$.

In the case $m = 3$ of the paper we simply had

$$X_1 = \log \left|\zeta_1^{1/2}\zeta_1^{(1)}\right| \quad \text{and} \quad X_2 = \log \left|\zeta_2^{1/2}\zeta_2^{(1)}\right|$$

and the assertion was easy to establish. However if $m = 4$ we would need the three 2×2-minors of

$$\begin{pmatrix} \log \left|\zeta_1^{1/3}\zeta_1^{(1)}\right| & \log \left|\zeta_2^{1/3}\zeta_2^{(1)}\right| & \log \left|\zeta_3^{1/3}\zeta_3^{(1)}\right| \\ \log \left|\zeta_1^{1/3}\zeta_1^{(2)}\right| & \log \left|\zeta_2^{1/3}\zeta_2^{(2)}\right| & \log \left|\zeta_3^{1/3}\zeta_3^{(2)}\right| \end{pmatrix} \tag{22}$$

to be linearly independent over $\mathbf{Q}$. We note that the above matrix is a piece of the regulator matrix for K modified by elementary row operations and thus has rank = 2 and so at least one minor is nonzero. Suppose in (22) $k_1 \neq 0$, k_2, k_3 are integers such that

$$k_1 \det(X_1, X_2) + k_2 \det(X_2, X_3) + k_3 \det(X_3, X_1) = 0.$$

Then

$$\det(k_1X_1-k_2X_3,\ k_1X_2-k_3X_3)=0.$$

One checks immediately that

$$\zeta_1^{k_1}\zeta_3^{-k_2} \quad \text{and} \quad \zeta_2^{k_1}\zeta_3^{-k_3}$$

are independent units. So it would suffice to show: *Let* ζ_1, ζ_2 *be any two independent units in a totally real field of degree* 4 *over* $\mathbf{Q}$. *Then*

$$\begin{pmatrix} \log|\zeta_1^{1/3}\zeta_1^{(1)}| & \log|\zeta_2^{1/3}\zeta_2^{(1)}| \\ \log|\zeta_1^{1/3}\zeta_1^{(2)}| & \log|\zeta_2^{1/3}\zeta_2^{(2)}| \end{pmatrix}$$

is nonsingular.

Now let us suppose that the analogue of Lemma 7 has been proved. Lemma 10 would then be valid as stated. But one key point in the proof was that ξ_v and q_v had the same order of magnitude for those v satisfying our conditions. To do this we had to have that $q_v \neq 0$ (see Lemma 4) and this was proved in Lemma 3 by applying Thue's theorem. The corresponding result to Lemma 3 is trivially not true in higher dimensions (see [2]; page 299). However Lemma 3 is much more than we need. Assuming Lemma 7 and hence Lemma 10 we see the v satisfying our conditions form a one parameter family and so for these v, probably $q_v \neq 0$.

7. What Happened to the Error Term?

The error term disappeared in Lemma 7 (the rest of the proof could be altered to produce one if we had one in Lemma 7) when we applied the uniform distribution theorem to, say in Case I,

$$\theta=\frac{\log|\zeta_1^{1/2}\zeta_1^{(1)}|}{\log|\zeta_2^{1/2}\zeta_2^{(1)}|}.$$

Applying the result ([6]; page 28); if one had a good "type" for θ, i.e. irrationality measure, one could give an error term in Lemma 7.

Suppose θ has type $\leq g$ (so g = an increasing function such that $|q\theta-p| < 1/qg(q)$ has only a finite number of solutions). Then from [6]

$$\#_N = C_5N+O\left(\int_1^N (g(t)^{1/2}/t^{1/2})\,dt\right).$$

Then we would obtain

$$\lambda_B = C'\log B+O\left(\int^{C_9\log B} (g(t)^{1/2}/t^{1/2})\,dt\right).$$

So if for example $g(t)=t^{1/2}$ (in terms of diophantine approximations a rather crude type) we would have an error of $O(\log^{3/4} B)$. However the

best type so far known for numbers like θ have the order of magnitude (see [4]; page 175)

$$g(t) = \underline{e}^{\log^{2+\varepsilon} t}$$

much too crude to give an error term.

Finally the same analysis using [1] would yield an error term in the higher dimensional case if one could obtain a sufficiently good linear independence measure for the determinants of the conjecture of the last section.

References

1. Adams, W. W. Simultaneous asymptotic diophantine approximations. *Mathematika* **14** (1967), 173–180.
2. Borevich, Z. I. and Shafarevich, I. R. "Number Theory". Academic Press, New York, 1966.
3. Cassels, J. W. S. "An Introduction to Diophantine Approximations". Cambridge University Press, Cambridge, 1957.
4. Gelfond, A. O. "Transcendental and Algebraic Numbers". Dover, New York, 1960.
5. Lang, S. "Algebraic Numbers". Addison–Wesley, Reading, Mass., 1964.
6. Lang, S. "Introduction to Diophantine Approximations". Addison–Wesley, Reading, Mass., 1966.
7. LeVeque, W. J. "Topics in Number Theory", vol. II. Addison–Wesley, Reading, Mass., 1956.
8. Schmidt, W. M. A Metrical Theorem in Diophantine Approximations. *Canadian J. Math* **11** (1960), 619–631.
9. Schmidt, W. M. Simultaneous approximations to a basis of a real algebraic number field. *Am. J. Math.* **88** (1966), 517–527.